



Homeland Security

Daily Open Source Infrastructure Report

15 June 2015

Top Stories

- An audit of 12 Massachusetts State agencies released June 11 uncovered a failure to comply with State requirements regarding the removal of sensitive information from electronic equipment. – *Boston State House News Service* (See item [18](#))
- New York officials reported June 12 that an employee at the New York Clinton Correctional Facility allegedly provided equipment used in the escape of two convicted murderers June 6. – *CNN* (See item [19](#))
- Researchers discovered that Apple Watch users running watchOS 1.0 are vulnerable to attacks in which threat actors can leverage Internet Control Message Protocol to potentially steal credentials and deliver malicious payloads. – *Softpedia* (See item [22](#))
- Researchers reported an unpatched vulnerability in the firmware code of N-Tron 702W industrial-level wireless access point systems in which an attacker could use secure shell to remotely intercept encryption keys and communication from the device. – *Softpedia* (See item [23](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. ***June 11, San Antonio Business Journal*** – (Texas) **Report: \$197,000 worth of crude oil released into air during Encana accident.** Encana Corp., released findings from a report in the week of June 2 into a May oil rig accident near Karnes City, Texas, revealing that approximately 138,000 gallons of crude oil spilled from the Droomgoole B 8H oil well, resulting in the release of 760,956 pounds into the air along with 18 other different types of gases.

Source: <http://www.bizjournals.com/sanantonio/blog/eagle-ford-shale-insight/2015/06/report-197-000-worthof-crude-oil-released-into-air.html>

For additional stories, see items [23](#) and [26](#)

[\[Return to top\]](#)

Chemical Industry Sector

2. ***June 10, U.S. Department of Labor*** – (Texas) **Workers exposed to physical injury, amputation risks at chemical manufacturing facility.** The Occupational Safety and Health Administration cited Venture Chemicals Inc., June 10 for 18 serious and 9 other-than-serious safety violations after an employee was fatally caught in an auger bin late 2014. Proposed penalties total \$63,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28122
3. ***June 10, WPSD 6 Paducah*** – (Kentucky) **All clear given in anhydrous ammonia gas leak in Mayfield, Kentucky.** Kentucky State Police reported June 10 that an anhydrous ammonia gas leak at Providence Ag in Mayfield sent two people to area hospitals after a fitting ruptured when crews were filling a tank with the gas. HAZMAT crews cleared the incident and an investigation is ongoing.
Source: <http://www.wpsdlocal6.com/story/29286522/anhydrous-ammonia-gas-leak-in-mayfield-kentucky>

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

See items [23](#) and [26](#)

[\[Return to top\]](#)

Critical Manufacturing Sector

4. ***June 11, International Business Times*** – (National) **Acura recalls 48,000 MDX and RLX SUV models due to automatic braking system glitch.** Honda Motor Co. Ltd., issued a recall June 11 for 48,000 model year 2014 – 2015 Acura MDX and RLX

SUVs worldwide due to a glitch in the “Collision Mitigation Braking System” in which vehicles could suddenly brake aggressively instead of slowing down when detecting another vehicle accelerating in front while driving along an iron fence or metal guardrail.

Source: <http://www.ibtimes.com/acura-recalls-48000-mdx-rlx-suv-models-due-automatic-braking-system-glitch-1962068>

5. ***June 11, York Daily Record*** – (Pennsylvania) **Fire at Pennex Aluminum in Wellsville halts production, forces evacuation.** Fifty firefighters and fire police from 4 counties responded to a 2-alarm fire at Pennex Aluminum in Wellsville, Pennsylvania, June 11 that prompted the evacuation of about 80 employees and reportedly started in the engine compartment of a front-end loader. Officials are unsure of exact damages suffered, and an investigation is ongoing.

Source: http://www.ydr.com/local/ci_28294140/york-county-911-crews-responding-fire-wellsville

6. ***June 10, U.S. Department of Labor*** – (Florida) **Contender Boats continues to expose workers to fall, amputations and electrical hazards.** The Occupational Safety and Health Administration cited Homestead, Florida-based Contender Boats Inc., with 25 safety and health violations June 10 for continually allowing the operation of forklifts with broken seats, failing to perform frequent inspections of cranes, exposing workers to an unsecured drill press, and other hazards. Proposed penalties total \$106,000.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28119

For another story, see item [26](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

7. ***June 10, U.S. Department of Labor*** – (Hawaii) **OSHA orders safety upgrades after 7-ton buoy hits, kills 2 workers and injures 2 others at Pearl Harbor naval facility.** The Occupational Safety & Health Administration cited the Naval Inactive Ships Maintenance Office in Honolulu, Hawaii, June 10 for 5 safety violations following a December 2014 incident in which a 7-ton buoy killed 2 workers and injured 2 others. Proposed fines total \$46,000.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28125

[\[Return to top\]](#)

Financial Services Sector

See item [18](#)

[\[Return to top\]](#)

Transportation Systems Sector

8. ***June 12, Pittsburgh Post-Gazette*** – (Pennsylvania) **Pittsburgh woman killed in three-vehicle crash on Route 28 in Shaler.** Route 28 in Shaler was shut down for about 3 hours June 11 due to a 3-vehicle accident that killed 1 person and injured 3 others. Source: <http://www.post-gazette.com/news/transportation/2015/06/11/One-injured-in-crash-on-Route-28-near-Millvale-exit/stories/201506110205>
9. ***June 11, KCNC 4 Denver*** – (Colorado) **I-70 reopens after rock slide in Glenwood Canyon.** Interstate 70 in Gypsum reopened June 11 after being closed for approximately 7 hours while crews cleared the debris and inspected the road for any damage following a rock slide in Glenwood Canyon. No injuries were reported. Source: <http://denver.cbslocal.com/2015/06/11/backups-result-from-rock-slide-in-glenwood-canyon/>
10. ***June 11, WAVE 3 Louisville*** – (Kentucky) **1 seriously injured in I-71 rollover crash.** Northbound lanes of Interstate 71 at mile marker 4 in Louisville was shut down for approximately 2 hours June 11 due to a single-vehicle crash that tore out a section of the guardrail and injured 1 person. Source: <http://www.wave3.com/story/29300194/i-71-north-closed-near-watterson-due-to-rollover-crash>
11. ***June 11, Los Angeles Daily News*** – (California) **2 seriously injured in head-on crash on Pacific Coast Highway in Malibu.** The Pacific Coast Highway in Malibu was shut down for more than 8 hours June 10 due to a head-on crash that seriously injured 2 people. The cause of the crash remains under investigation. Source: <http://www.dailynews.com/general-news/20150611/2-seriously-injured-in-head-on-crash-on-pacific-coast-highway-in-malibu>

For additional stories, see items [18](#) and [23](#)

[\[Return to top\]](#)

Food and Agriculture Sector

12. ***June 12, Associated Press*** – (Michigan) **10,000 chickens die in Michigan barn fire.** Authorities reported June 12 that an overnight fire at a Bronson Township barn killed approximately 10,000 chickens while heavily damaging the barn June 9 – 10. Fire crews contained the incident and no injuries were reported. Source: <http://www.freep.com/story/news/local/michigan/2015/06/12/chickens-die-michigan-barn-fire/71109942/>
13. ***June 11, KPHO 5 Phoenix; KTVK 3 Phoenix*** – (Arizona) **Bird flu in Arizona? 4 AZ facilities quarantined.** The U.S. Department of Agriculture reported June 11 that 4

counties in Arizona may have been infected with the bird flu after initial test results showed positive traces of the disease. Officials have quarantined the birds until further testing can be done.

Source: <http://www.kpho.com/story/29301321/bird-flu-in-arizona-4-az-facilities-quarantined>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

14. ***June 11, WBKO 13 Bowling Green*** – (Kentucky) **Morgantown Utilities boil water advisory.** Morgantown Utilities in Kentucky has issued a boil water advisory for most of its customers from June 11 through June 12 while crews connect newly installed lines and valves in the area.

Source: <http://www.wbko.com/home/headlines/Morgantown-Utilities-Boil-Water-Advisoy-306961791.html>

For additional stories, see items [23](#) and [26](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

15. ***June 11, Associated Press*** – (Texas) **Texas Medicaid patients have private data exposed online.** The Texas Department of Aging and Disability Services reported June 11 that approximately 6,600 Medicaid recipients' records containing personal identifiable information (PII) and treatment information were compromised in a data breach discovered in April 2015 after an internal Web application was made public. The Web site was taken down, and none of the information has been misused.

Source: <http://newsok.com/texas-medicaid-patients-have-private-data-exposed-online/article/feed/850949>

16. ***June 11, Bakersfield Californian*** – (California) **Fire at Ridgecrest Regional Hospital causes more than \$15,000 in damage.** Two adults suffered minor smoke inhalation after a mechanical failure at Ridgecrest Regional Hospital caused a compressor to catch fire on the second floor of a building June 11. Firefighters estimated over \$15,000 in damages.

Source: <http://www.bakersfield.com/local/breaking-news/2015/06/11/fire-at-ridgecrest-regional-hospital-causes-more-than-15-000-in-damage.html>

17. ***June 10, Business Wire*** – (Indiana) **Medical Informatics Engineering notifies patients of a data security compromise.** Medical Informatics Engineering announced June 10 it had been targeted by a sophisticated cyber-attack which compromised the sensitive health information of patients affiliated with several of its clients, including Concentra, Fort Warne Neurological Center, Franciscan St. Francis Health Indianapolis, Gynecology Center, Inc. Fort Wayne, and Rochester Medical Group, as well as clients associated with the company's subsidiary NoMoreClipboard. The

incident is currently under investigation.

Source: <http://www.businesswire.com/news/home/20150610005961/en/Medical-Informatics-Engineering-notifies-Patients-Data-Security#.VXrkLkbajU>

For another story, see item [18](#)

[\[Return to top\]](#)

Government Facilities Sector

18. ***June 11, Boston State House News Service*** – (Massachusetts) **Auditor: 12 agencies failed to properly handle sensitive computer records.** An audit of 12 Massachusetts State agencies released June 11 uncovered a failure to comply with State requirements regarding the removal of sensitive information from electronic equipment. State agencies faulted included the Office of the Chief Medical Examiner, The Massachusetts State Police, the State Lottery Commission, the Department of Public Health, and 8 others.
Source: http://www.masslive.com/news/index.ssf/2015/06/auditor_12_agencies_failed_to_o.html

[\[Return to top\]](#)

Emergency Services Sector

19. ***June 12, CNN*** – (New York) **New York prison employee gave blades, drill bits to escapees, sources say.** The Clinton County District Attorney reported June 12 that an employee at the New York Clinton Correctional Facility allegedly provided equipment including hacksaw blades, drill bits, and eyeglasses with light fixtures, used in the escape of two convicted murderers June 6. An investigation is ongoing to find the escaped prisoners.
Source: <http://www.cnn.com/2015/06/12/us/new-york-prison-break/index.html>
20. ***June 11, Miami Herald*** – (Florida) **Fla. corrections officers allegedly beat inmate.** Two former officers at Florida's Franklin Correctional Institution were indicted June 10 by a Federal grand jury for allegedly conspiring to violate the civil rights of a State inmate and for depriving the inmate of constitutional rights in July 2014.
Source: <http://www.officer.com/news/14000075/florida-corrections-officers-allegedly-beat-inmate>

For additional stories, see items [18](#) and [30](#)

[\[Return to top\]](#)

Information Technology Sector

21. *June 12, Softpedia* – (International) **44.5 million new malware variants recorded in 1 month.** Symantec released findings from a report revealing that new malware variants increased by over 50 percent in May to 44.5 million, that the most commonly seen threat on the Apple OS X operating system (OS) was a trojan virus that changes the domain name system settings of affected computers, and that medium-sized companies were the most frequently targeted by spear-phishing attacks.
Source: <http://news.softpedia.com/news/44-5-Million-New-Malware-Variants-Recorded-in-1-Month-484138.shtml>
22. *June 12, Softpedia* – (International) **Apple fixed a nasty MitM vulnerability in the latest watchOS.** Security researchers from Zimperium Mobile Security discovered that Apple Watch users running watchOS 1.0 are vulnerable to man-in-the-middle attacks dubbed “DoubleDirect” in which threat actors can leverage Internet Control Message Protocol (ICMP) redirects from the device and gateway to potentially steal credentials and deliver malicious payloads that could spread to devices on an entire corporate network.
Source: <http://news.softpedia.com/news/Apple-Fixed-a-Nasty-MitM-Vulnerability-in-the-Latest-watchOS-484117.shtml>
23. *June 11, Softpedia* – (International) **Encryption keys hard-coded in industrial access point.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported an unpatched vulnerability in the firmware code of N-Tron 702W industrial-level wireless access point systems in which an attacker could use secure shell (SSH) to remotely intercept encryption keys and communication from the device.
Source: <http://news.softpedia.com/news/Encryption-Keys-Hard-Coded-in-Industrial-Access-Point-484073.shtml>
24. *June 11, Softpedia* – (International) **Fileless malware makes almost 200,000 victims mostly in the U.S.** Security researchers at Symantec discovered that cybercriminals used a Microsoft Windows zero-day vulnerability permitting arbitrary remote file execution to spread Poweliks malware to 198,500 computers, almost all of which were in the U.S. Poweliks resides in system memory and is primarily used for ad-fraud purposes.
Source: <http://news.softpedia.com/news/Fileless-Malware-Makes-Almost-200-000-Victims-Mostly-In-the-US-484030.shtml>
25. *June 11, Softpedia* – (International) **CryptoWall 3.0 delivered in campaign started more than a week ago.** Security researchers from Cisco’s TALOS discovered an active malicious email campaign purporting to be regarding possible employment including hypertext markup language (HTML) attachments that redirect users to Google Drive accounts hosting the CryptoWall ransomware.
Source: <http://news.softpedia.com/news/CryptoWall-3-0-Delivered-In-Campaign-Started-More-Than-A-Week-Ago-484046.shtml>
26. *June 11, Securityweek* – (International) **Only few organizations patched recent**

Honeywell SCADA flaw: researchers. Security researchers from Outpost24 reported that 90 Honeywell Falcon XLWeb supervisory control and data acquisition (SCADA) control systems, most located in Europe and the Middle East, remain unpatched and are vulnerable to directory traversal flaws in which an attacker could execute operating system (OS) commands. The experts believe that four of the systems analyzed could have been exploited.

Source: <http://www.securityweek.com/only-few-organizations-patched-recent-honeywell-scada-flaw-researchers>

27. *June 11, Securityweek* – (International) **OpenSSL patches Logjam bug, DoS vulnerabilities.** OpenSSL released patches for its open-source toolkit addressing the “Logjam” vulnerability in which an attacker could use a man-in-the-middle (MitM) attack to force transport layer security (TLS) connections to downgrade to weaker cryptography, as well as a denial-of-service (DoS) vulnerability caused by the way ECParameters structures are handled.

Source: <http://www.securityweek.com/openssl-patches-logjam-bug-dos-vulnerabilities>

For additional stories, see items [15](#), [17](#), and [18](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

See item [22](#)

[\[Return to top\]](#)

Commercial Facilities Sector

28. *June 12, Associated Press* – (Connecticut) **Nine people shot at Conn. Housing complex.** A June 11 shooting at the Trumbull Gardens complex in Bridgeport, Connecticut, left 1 man dead and 8 others injured when 2 men opened fire on a group of people in the complex’s parking lot. Authorities contained the incident and increased police patrols in the area.

Source: <http://www.officer.com/news/14001818/nine-people-shot-at-conn-housing-complex>

29. *June 12, KYW 3 Philadelphia* – (Pennsylvania) **Investigation continues into Delco Apartment fire that displaced dozens.** A 2-alarm fire prompted the evacuation of approximately 80 residents June 11 at the Strafford Court Apartment complex in

Lansdowne, Pennsylvania, after the blaze began in the complex basement. Two people were injured and sent to area hospitals and an investigation is ongoing to determine the cause of the fire.

Source: <http://philadelphia.cbslocal.com/2015/06/12/investigation-continues-into-delco-apartment-fire-that-displaced-dozens/>

30. ***June 11, CBS News; Associated Press* – (Massachusetts) **1 dead, 11 hospitalized in apparent suicide by chemicals.**** Lowell police reported June 11 that a Lowell, Massachusetts man released several chemical gasses in his apartment after being distraught over a failing relationship. The incident killed the man and sent 11 people to area hospitals, including 4 police officers and 3 emergency medical workers.

Source: <http://www.cbsnews.com/news/1-dead-11-hospitalized-in-apparent-suicide-by-chemicals-in-massachusetts/>

For another story, see item [23](#)

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.